

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

JUNIPER NETWORKS, INC.,
Petitioner,

v.

MONARCH NETWORKING SOLUTIONS LLC,
Patent Owner.

U.S. Patent No. 8,693,369

“Method of Routing a Data Packet in a Network and an Associated Device”

IPR2024-00175

PETITIONER’S REPLY TO PATENT OWNER RESPONSE

I.	INTRODUCTION	1
II.	ARGUMENT.....	2
A.	Ground 1: Patent Owner Forfeits a Response to Petitioner’s Arguments	2
B.	Grounds 2 and 4: Fangman’s NAPPT, in view of Kumar, Teaches the ’369 Patent’s “Port Masks”	5
1.	Patent Owner Misunderstands Fangman and the Technology at Issue	5
(a)	Patent Owner’s Interpretation Rests on a Technical Misunderstanding of NAT and IP Telephones.....	9
(b)	Patent Owner Forfeits the Board’s Interpretation, Which Is Also Contradicted by Fangman and Is Inefficient.....	15
2.	As the Board Has Already Recognized, a POSITA Would Have Found It Obvious to Combine Fangman with Kumar	17
C.	Grounds 3 and 5: A POSITA Would Have Found It Obvious to Apply King’s Outbound Teachings to Inbound Communications.....	20
1.	Patent Owner Recognizes That King Uses Port Ranges to Identify User Devices and Provides No Reason Why This Teaching Is Limited to Outbound Communications	20
2.	As the Board Has Already Recognized, a POSITA Would Have Found It Obvious to Combine King with Kumar.....	23
III.	CONCLUSION.....	24

PETITIONER'S EXHIBIT LIST

EX1001	U.S. Patent No. 8,693,369 to Mohamed Boucadair (“’369 patent”)
EX1002	Prosecution history of U.S. Patent No. 8,693,369 (“’369 Prosecution History”)
EX1003	Declaration of Dr. Samrat Bhattacharjee under 37 C.F.R. §1.68
EX1004	<i>Curriculum Vitae</i> of Dr. Bhattacharjee
EX1005	Declaration of Dr. Sylvia Hall-Ellis under 37 C.F.R. §1.68
EX1006	P. Richter et al., “A Primer on IPv4 Scarcity,” (Feb. 27, 2015), available at https://arxiv.org/pdf/1411.2649.pdf
EX1007	H. Yeom et al., “IP Multiplexing by Transparent Port-Address Translator,” 10th USENIX System Administration Conference (LISA X) (Sept. 29, 1996), available at https://www.usenix.org/conference/lisa-96/ip-multiplexing-transparent-port-address-translator
EX1008	RFC 3022 (Traditional NAT), dated January 2001, available at https://datatracker.ietf.org/doc/html/rfc3022
EX1009	U.S. Patent Application Publication No. 2002/0016826 to Johansson et al. (“Johansson”)
EX1010	A. Reitz, “The Dynamic Port Reservation Protocol,” Univ. Ill. at Urbana-Champaign (2001), available at http://redefine.dyndns.org/~andyr/documents_and_writings/thesis/docs/areitz_msthesis.pdf
EX1011	M. Shin et al., “Using a Single IPv4 Global Address in DSTM,” Internet Engineering Task Force (“IETF”) (Feb. 22, 2001), available at https://www.ietf.org/archive/id/draft-shin-dstm-single-ipv4-00.txt (“Shin”)
EX1012	U.S. Patent No. 7,356,045 to Satapati et al. (“Satapati”)
EX1013	U.S. Patent Application Publication No. 2003/0154306 to Perry (“Perry”)

EX1014	RFC 950 (Internet Standard Subnetting Procedure), dated August 1985, available at https://datatracker.ietf.org/doc/html/rfc950
EX1015	U.S. Patent No. 7,624,195 to Biswas et al. ("Biswas-195")
EX1016	WO Publication No. 01/02965 A2 to Herbst et al. ("Herbst")
EX1017	RFC 7597 (Mapping of Address and Port with Encapsulation), dated July 2015, available at https://datatracker.ietf.org/doc/html/rfc7597
EX1018	RFC 4632 (Classless Inter-domain Routing), dated August 2006, available at https://datatracker.ietf.org/doc/html/rfc4632
EX1019	U.S. Patent Application No. 10/873,547 to Tornetta et al. ("Tornetta")
EX1020	U.S. Patent No. 7,873,038 to LaVigne et al. ("LaVigne")
EX1021	U.S. Patent Application No. 11/699,765 to McAlister ("McAlister")
EX1022	U.S. Patent No. 8,019,889 to Biswas et al. ("Biswas")
EX1023	U.S. Patent No. 7,394,809 to Kumar et al. ("Kumar")
EX1024	U.S. Patent No. 7,068,647 to Fangman et al. ("Fangman")
EX1025	U.S. Patent No. 8,032,639 to King et al. ("King")
EX1026	RFC 791, Internet Protocol Specification (September 1981), available at https://datatracker.ietf.org/doc/html/rfc791
EX1027	U.S. Patent No. 5,014,221 to Mogul ("Mogul")
EX1028	U.S. Patent No. 5,163,131 to Row et al. ("Row")
EX1029	July 20, 2006 Capture of RFC 791, Wayback Machine, available at https://web.archive.org/web/20060720182319/http://www.ietf.org/rfc/rfc791.txt
EX1030	Michael Witt, A Comment on Current Source Routing Techniques (1987), available at https://dl.acm.org/doi/pdf/10.1145/36727.36728

EX1031	Andrew Tanenbaum, <i>Computer Networks</i> (5th Ed. 2011)
EX1032	Monarch's Opposition to Juniper's Motion to Transfer, <i>Monarch Networking Solutions LLC v. Juniper Networks, Inc.</i> , No. 1:23-cv-670-TSE-LRV (E.D. Va. Oct. 3, 2023), ECF No. 52
EX1033	PTO Reexamination Operational Statistics, available at https://www.uspto.gov/learning-and-resources/statistics/reexamination-information
EX1034	Complaint, <i>Monarch Networking Solutions LLC v. Juniper Networks, Inc.</i> , No. 1:23-cv-670-TSE-LRV (E.D. Va. May 23, 2023), ECF No. 1
EX1035	Unified EPR (Control No. 90/015,315), filed on October 23, 2023
EX1039	Supplemental Declaration of Dr. Samrat Bhattacharjee under 37 C.F.R. §1.68
EX1040	Y. Miyazaki et al., <i>A Proposal for a NAT Traversal System That Does Not Require Additional Functions at Terminals</i> , IEEE (Oct. 2007), available at https://ieeexplore.ieee.org/abstract/document/4428885
EX1041	W. Jiang et al., <i>Towards Junking the PBX: Deploying IP Telephony</i> , Columbia Univ. (2001), available at https://www.cs.columbia.edu/~hgs/papers/Jian0106_Junking.pdf
EX1042	T. Wallingford, <i>Switching to VoIP</i> , O'Reilly (2005).
EX1043	P. Engelstad & G. Egeland, <i>Peer-to-Peer IP Telephony</i> , 102 <i>Teletronikk</i> 1 (2006), available at https://www.telenor.com/wp-content/uploads/2012/05/T06_1.pdf
EX1044	Y. Yu et al., <i>An Efficient NAT Traversal for SIP and Its Associated Media Sessions</i> , Int'l Comp. Symposium (Dec. 15-17, 2004), available at http://dspace.fcu.edu.tw/bitstream/2377/1829/1/ce07ics002004000150.pdf

EX1045	F. Thernelius, <i>SIP, NAT, and Firewalls</i> , Royal Institute of Tech. Stockholm (May 2000), available at https://www.cs.columbia.edu/sip/drafts/Ther0005_SIP.pdf
EX1046	Andrew Tanenbaum, <i>Computer Networks</i> (4th Ed. 2003)

I. INTRODUCTION

Patent Owner makes fatal technical mistakes in responding to all of Petitioner's grounds. Regarding ground 1, Patent Owner overlooks that the '369 claims are directed to *inbound* transmissions, and focuses instead on Biswas's *outbound* teachings. Patent Owner ignores and therefore concedes that Biswas teaches the '369 patent's inbound claims.

Regarding ground 2, Patent Owner incorrectly assumes that the service gateway in Fangman uses "traditional NAT or PAT" to route inbound data packets, in which "the service gateway checks whether the persistent port number in the destination packet matches the port number used by the IP telephone in *a prior outgoing transmission*." Paper 15 ("POR"), at 13, 22 (emphasis added). Patent Owner fails to realize that relying on "a prior outgoing transmission" would break IP telephone networks globally by freezing them in a never-ending stasis, like neighbors that refuse to introduce themselves unless the other does it first. For this very reason, Fangman disavowed the use of traditional NAT in IP telephone networks and invented NAPPT to replace it, which uses port ranges instead of a "prior outgoing transmission" to overcome this "you first" problem.

Regarding ground 3, Patent Owner admits that King teaches using port ranges to "identify[] a source device" when routing outbound transmissions, (POR 27), but Patent Owner says this teaching is not enough because the '369 patent focuses

instead on inbound transmissions. In the context of King, however, the inbound and outbound processes are so functionally identical that reversing the process requires replacing only one variable: `received_source_port` with `received_destination_port`. Thus, King did not need to detail the inbound process because doing so would have been redundant; a POSITA would have known how to implement inbound transmissions based on King's outbound disclosures.

All of the '369 patent's claims are therefore invalid as obvious, and Petitioner respectfully asks the Board to cancel these claims.

II. ARGUMENT

A. Ground 1: Patent Owner Forfeits a Response to Petitioner's Arguments

As a preliminary matter, Patent Owner analyzes only dependent claims 8 and 12. POR 16-19. Petitioner's analysis of the other claims in this ground therefore stands unopposed, leaving only claims 8 and 12. *Viking Drill & Tool, Inc. v. Wang*, IPR2023-00474 (PTAB July 5, 2024), Paper 89, at 22 ("In an *inter partes* review, arguments not made or insufficiently developed are forfeit.") (citing cases).

Patent Owner's arguments regarding claims 8 and 12 fail because claims 8 and 12 are directed to ***inbound*** transmissions and the petition showed that Biswas teaches these ***inbound*** transmissions, yet Patent Owner's response ignores inbound transmissions entirely and instead analyzes only ***outbound*** transmissions. Petitioner's argument therefore stands unopposed. EX1039 ¶¶3-8. Even if the

Board were to generously allow Patent Owner to apply its outbound analysis to inbound transmissions, Patent Owner would still be incorrect on the merits. Claims 8 and 12 are thus invalid under ground 1.

Claims 8 and 12 explicitly limit themselves to transmissions that are inbound to the private network. *Id.* ¶¶3-7. Both claims require “a data packet comprising said primary address *as the destination address* to said piece of terminal equipment.” EX1001, claims 8, 12 (emphasis added). The primary address serves as a destination address only for inbound transmissions. EX1039 ¶¶4-5. Claims 8 and 12 are therefore limited to data packets *entering* a private network (*i.e.*, inbound transmissions). *Id.* ¶¶6-7. In fact, this is exactly how Petitioner analyzed Biswas and claims 8 and 12 in the petition. Paper 1 (“Petition”), at 27-28, 33-34; *see also* EX1039 ¶¶8-9.

Despite both the '369 patent and the petition focusing solely on inbound transmissions, Patent Owner ignores inbound transmissions and discusses only irrelevant outbound transmissions in its response. Specifically, Patent Owner argues that “[t]he host **102**...uses the address as a *source* address for a packet sent out of the private network”; “the global address identifies either the host **102** or edge router **104** (*the source of the packet*), not master gateway **110**”; and “[n]othing else in Biswas suggests that the Global Address could identify gateway master **110 to host**

102, edge 104, or any other device on the private network.” POR 19 (emphasis added).

Patent Owner’s argument is wrong. Even within a private network, a host can use a global address to communicate with the gateway master, as Petitioner’s technical expert has confirmed using real-world experimentation. EX1039 ¶10. But more importantly, Patent Owner’s framing of the issue as an outbound issue in which the address is used as a source address is incorrect. *See id.* ¶¶3-7. The proper framing is whether a device on the public network, like host **118**, can identify gateway master **110** using the global address (*i.e.*, in an inbound transmission), not whether a device on the private network, like host **102**, can identify gateway master using the global address (*i.e.*, in an outbound transmission). *See id.* Patent Owner therefore fails to address what is actually at issue in claims 8 and 12 as well as Petitioner’s analysis of these claims in view of Biswas, which stand unopposed.

The Board should reject any belated attempt by Patent Owner to discuss outbound transmissions in sur-reply. Patent Owner “forfeited” any argument addressing inbound transmissions “by not raising it in the Patent Owner Response.” *Google LLC v. Ecofactor, Inc.*, IPR2022-00473 (PTAB Aug. 1, 2023), Paper 25, at 44. Allowing Patent Owner to make these belated arguments in sur-reply would prejudice Petitioner by depriving it an opportunity to respond to Patent Owner’s exact assertions.

Even if the Board were to allow Patent Owner to argue that the global address does not identify gateway master **110** for inbound transmissions, this argument still fails on the merits. For the inbound transmissions discussed above, the global address *must* identify gateway master **110**. EX1039 ¶9. Otherwise, gateway master **110** would not receive inbound data packets that use the global address as the destination address. *Id.* Applying Patent Owner's argument to inbound transmissions is like arguing an address "does not identify" a home even though (1) the address is assigned to that home and (2) all letters marked with that address are delivered to that home. Arguing that the gateway master is not identifiable by a global address would also contradict Biswas's disclosure that the gateway master acts as a NAT device because it was known in the art that NAT devices *are* identifiable by a global address. *Id.*

Claims 7-14 and 16-17 are therefore invalid as obvious under ground 1.

B. Grounds 2 and 4: Fangman's NAPPT, in view of Kumar, Teaches the '369 Patent's "Port Masks"

1. Patent Owner Misunderstands Fangman and the Technology at Issue

The crux of the dispute between the parties comes down to how Fangman implements and utilizes the disclosed "table of semi-permanent mappings of the external IP address and ports to the internal hosts and ports." EX1024, 8:49-51. In Petitioner's view, Fangman discloses that the service gateway stores port range

assignments during initialization and uses those port ranges to route inbound data packets. *See* EX1039 ¶¶16, 19. For example, the service gateway may store the following in a table for one of the IP telephones in the private network:

Private Address	Public Address	Assigned Port Range
10.255.255.123	31.31.98.152	8,192-8,447 ¹

Id. ¶23. Patent Owner's view, on the other hand, is that the service gateway relies on port range assignments simply to verify that hosts are using the correct ports for outbound data packets and then uses a process "similar to traditional NAT or PAT"²

¹ If implementing a port mask instead of a port range, then this cell would contain the appropriate port mask. EX1039 ¶23 n.5.

² As used here, "traditional NAT" refers to the process of maintaining a connection-state table and using that table to route inbound data packets. EX1039 ¶11 n.1. Fangman uses the more general terms "NAT" or "NAPT" to refer to the generic process of translating a private IP address into a public IP address and vice versa, which might or might not involve translating addresses via a connection-state table. *See, e.g.*, EX1024, 8:52-54 ("The SG **170** may continue to replace the internal or private source IP address with the NATed external source IP address."); EX1024, 10:61-62 (explaining that the service gateway can "[p]rovide basic NAT translation (private to public IP) without changing port number"); EX1024, 11:37 (explaining that the service gateway can "[a]ssign [a] NAT address"); EX1039 ¶11 n.1.

for inbound data packets, in which “the service gateway checks whether the persistent port number in the destination packet matches the port number used by the IP telephone in a prior outgoing transmission.” POR 13, 22 (emphasis omitted). In other words, Patent Owner asserts that the service gateway dynamically populates and de-populates a connection-state table as it routes inbound and outbound data packets, as in traditional NAT. Patent Owner’s argument is incorrect, resting on a fundamental misunderstanding of NAT and IP telephony and contradicting Fangman’s explicit disclosures. EX1039 ¶¶11-21. As Petitioner discusses in further detail below, traditional NAT can only handle inbound data packets that are solicited by a prior outbound data packet. *Id.* ¶¶12-15. IP telephones, on the other hand, must be able to handle unsolicited inbound communications without depending on prior outbound communications. *Id.* Fangman itself identifies this problem with NAT and describes it as a “[c]onsiderable problem[]” that its NAPPT intends to solve. EX1024, 2:54-65. Thus, Patent Owner’s argument does not make technical sense in light of the art and Fangman’s explicit disclosures.

The Board appears to have a third interpretation of Fangman,³ in which the service gateway persistently stores individual associations between a private

³ Petitioner addresses this interpretation even though Patent Owner has forfeited it by not raising it the Patent Owner Response.

address, private port number, public address, and public port number, and then uses a simple look up on an individual port number—rather than a port range—to route inbound data packets. Paper 12 (“ID”), at 24. Under the Board’s interpretation, Fangman would store, for example, the following persistent table for an IP telephone instead of Petitioner’s exemplary port-range table above:

Private Address	Internal Port	Public Address	External Port
10.255.255.123	8,192	31.31.98.152	8,192
10.255.255.123	8,193	31.31.98.152	8,193
10.255.255.123	8,194	31.31.98.152	8,193
...	...	...	...
10.255.255.123	8,447	31.31.98.152	8,447

EX1039 ¶23. Although the Board’s interpretation avoids Patent Owner’s technical mistake, it is inconsistent with Fangman’s teachings. *Id.* In several claims, like claim 1, Fangman discloses a “Service Gateway performing a network address persistent port translation (NAPPT) on the data packet,” which includes “storing translation information in a data structure” comprising three pieces of information: (1) “the private source IP address of the IP telephone,” (2) “a public IP address of the Service Gateway,” and (3) “*the assigned ports* for the IP telephone.” EX1024, 32:48-57 (emphasis added). Fangman thus teaches Petitioner’s port-range table shown above, not the Board’s proposed individual-port table. EX1039 ¶¶22-23. Further, a POSITA would have known that storing an individual-port table as opposed to a port-range table is inefficient and needlessly consumes a large amount of memory. *Id.* Instead of storing thousands, perhaps tens of thousands, of

individual rows—one for each assigned port number—the service gateway could instead store just a handful of port-range assignments. *Id.* Fangman therefore teaches using port ranges to route inbound data packets. *Id.* ¶¶11-24. At the very least, even if the Board were to conclude that Fangman teaches the individual-port implementation, a POSITA would have found it obvious to use a port-range implementation instead because it saves memory and is more efficient. *Id.* ¶¶22-23.

(a) Patent Owner's Interpretation Rests on a Technical Misunderstanding of NAT and IP Telephones

Patent Owner misunderstands the relevant technology when it asserts that Fangman uses a process “similar to traditional NAT or PAT” for inbound data packets, in which “the service gateway checks whether the persistent port number in the destination packet matches the port number used by the IP telephone in a prior outgoing transmission.” POR 13, 22 (emphasis omitted). To start, traditional NAT is incompatible with IP telephones. EX1039 ¶¶12-21. Traditional NAT works by maintaining a connection-state table in which internal hosts must first send an outbound data packet—which the NAT records in its database—before the NAT will accept an inbound data packet to that internal host. *Id.* ¶12. In other words, the internal host must first “solicit” a data packet before the NAT will let the data packet pass through. *Id.*

Traditional NAT's inability to handle “unsolicited” inbound transmissions makes it incompatible with IP telephony systems, which must be able to handle

unsolicited inbound transmissions so that telephones on the network can receive calls. *Id.* ¶¶13-15. As Fangman explains, “the resulting need to use Network Address Translation (NAT) and related technologies” and “the limitations of existing firewall technologies” were two of the “primary challenges” of IP telephony. EX1024, 1:36-46. “Complicating matters further, VoIP protocols often use pairs of ports for communication, initiated from both the inside *and outside* of the network. Firewalls^[4] tend to support single port communication *only initiated from the inside*,” *i.e.*, solicited inbound transmissions. EX1024, 2:12-27 (emphasis added). This unsolicited-transmissions issue was well known in the art prior to the ’369 patent’s invention. EX1039 ¶14 (discussing EXS1041-1045, which all confirm that NATs at the time of invention were incompatible with IP telephones).

Fangman describes this as a “[c]onsiderable problem[]” of NAT, (EX1024, 2:54-65), which it is: if Fangman were to use a process “similar to traditional NAT or PAT” that requires a “prior outgoing transmission,” (POR 13, 22), then the IP telephones in Fangman’s network would not be able to receive unsolicited inbound calls, (EX1039 ¶15). In fact, the telephones likely would not be able to make outbound calls either because, if the caller and recipient are both behind NATs, then

⁴ The service gateway in Fangman implements both the NAT and the firewall. EX1024, 8:44-57, 9:52-58.

the caller will not be able to place an outbound call to the recipient because the recipient's NAT would discard the call as an unsolicited inbound transmission. EX1039 ¶15. IP telephones would be at a stalemate, like two neighbors who refuse to introduce themselves to each other until the other does it first. Fangman thus discloses, and the prior art confirms, that traditional NAT is incompatible with IP telephony because of this “you first” problem.⁵ *Id.* Fangman therefore disavows traditional NAT and instead teaches an improvement to it, termed NAPPT. EX1024, 1:61-64, 2:66-67, 4:4-17.

Because IP telephones cannot rely on prior outbound transmissions, Fangman invented NAPPT to route inbound data packets based on port ranges. EX1039 ¶16. Fangman explicitly makes this point, explaining that “[i]nstead of dynamically assigning ports to IP telephones” as in traditional NAT, NAPPT “allocate[s] **a range** of port numbers for each IP telephone” and stores the port ranges in “a table of semi-permanent mappings.” EX1024, 8:45-67; *see also, e.g.*, EX1024, 3:25-37; EX1024, 11:14. NAPPT then handles inbound transmissions by “receiving a data packet from the IP device” that includes “a public destination IP address, a destination port

⁵ Fangman acknowledges that a solution to this problem exists, but Fangman disparages it as a “complex” and “convoluted process” that “introduc[es] substantial inefficiencies to the system.” EX1024, 2:54-65.

number *in the assigned range of port numbers*, and source information, where the public destination IP address and the destination port number may be used to uniquely identify the IP telephone.” EX1024, 4:18-25 (emphasis added). “The Service Gateway may then perform a Network Address Persistent Port Translation (NAPPT) on the data packet”—not traditional NAT—by consulting its table of port-range mappings, determining what “range of port numbers” the destination port falls into, and then routing the data packet based on the private address associated with that range of port numbers. *Id.* 4:25-27. Fangman accordingly explains that the service gateway stores “the assigned *ports* for the IP telephone” to perform the translation process. *Id.* 32:48-57 (emphasis added). By using port ranges, “the traditional problem of dynamic port numbers,” such as “[t]he problem of supporting application layer protocols that use UDP . . . and session[s] initiated from outside the network[,] may be addressed by the SG **170**” via “[t]he perpetual NAPT table maintained by the SG **170**.” *Id.* 14:9-14; *see also* EX1039 ¶16.

Other disclosures further confirm that Fangman relies on port ranges to route inbound data packets. EX1039 ¶¶17-19. Fangman discloses another hardware component, a media gateway controller, that the system uses to set up calls between IP telephones. EX1024, 2:43-53, 4:51-5:28. To establish these calls, the media gateway controller must be able to identify private addresses for IP telephones based on a public IP address and port number—just like the service gateway. EX1039 ¶19.

To make these identifications, the media gateway controller can “use the public IP address *and the port range* to determine the private IP address, for example, by using look-up tables.” EX1024, 3:53-64 (emphasis added).

Further, a POSITA would have generally understood that maintaining a connection-state table to route inbound data packets would be an inefficient use of memory. EX1039 ¶21. The service gateway is already “maintain[ing] a table of semi-permanent mappings of the external IP address and ports to the internal hosts and ports,” and it can route inbound packets according to the port ranges stored in this table. EX1024, 8:49-51; *see also* EX1024, 3:25-37 (“The Service Gateway may store the DHCP lease information” that contains “the range of port numbers . . . for the IP telephone.”); EX1024, 11:14 (“Assign port ranges for host, reserved in NAPT table.”). A POSITA would have therefore recognized that maintaining a separate connection-state table would be redundant and needlessly consume the router’s memory. EX1039 ¶21. The “table of semi-permanent mappings” is sufficient by itself. *Id.*

Patent Owner’s arguments to the contrary are incorrect. Fangman never says, as Patent Owner assumes, that it uses traditional NAT and relies on prior outbound transmissions to route inbound data packets. *Id.* ¶17. To the contrary, in the example provided in Figures 10A and 10B, a service gateway **170B** receives an inbound data packet and performs NAPPT on that inbound data packet without first sending a

prior outbound packet. *See* EX1024, 30:12-24, Figs. 10A-B; *see also* EX1039 ¶17. Further, Fangman emphasizes that the only reason to maintain a connection-state table, as used in traditional NAT, is to guarantee redundancy. EX1039 ¶18. As Fangman explains, “the primary SG **170** *may* maintain a connection state table for all NAT sessions” in order to ensure “*full redundancy* for each function that the SG **170** performs.” EX1024, 10:1-11 (emphasis added).

And Patent Owner is wrong to argue that “Fangman confirms that it uses only a port number” for routing inbound data packets because it discloses “using . . . ***the destination port number*** to uniquely identify the IP telephone.” POR 25 (emphasis in original). Here Patent Owner is trying to construe the phrase “using . . . the destination port number” to mean “exclusively relying on the destination port number.” But that is not the plain meaning of that phrase, much less how it is used in this disclosure. The verb “use” means “to employ for some purpose.” *Use*, Dictionary.com, available at <https://www.dictionary.com/browse/use> (last accessed Oct. 14, 2024); *see also Use*, Black’s Law Dictionary (14th ed. 2024) (“To employ for the accomplishment of a purpose.”). NAPPT “uses” or “employs” the destination port number to uniquely identify the IP telephone” when it compares the destination port number to the stored port range to determine the recipient host. EX1039 ¶20.

(b) Patent Owner Forfeits the Board's Interpretation, Which Is Also Contradicted by Fangman and Is Inefficient

The Board interpreted Fangman to store individual port assignments and then, “[w]hen the service gateway receives a data packet destined for the IP telephone” to “use[] the table to look up the private IP address of the telephone based on the port number, not the port range.” ID 24. Patent Owner does not adopt the Board's interpretation in its response, which is therefore waived. *See* Paper 13, at 9 (“Patent Owner is cautioned that any arguments not raised in the response may be deemed waived.”). Regardless, a POSITA would have recognized that maintaining or using a table that maps individual internal ports to individual external ports is also highly inefficient for the same reason. EX1039 ¶¶22-23. For example, Fangman could theoretically use the following table for routing inbound packets:

Private Address	Internal Port	Public Address	External Port
10.255.255.123	8,192	31.31.98.152	8,192
10.255.255.123	8,193	31.31.98.152	8,193
10.255.255.123	8,194	31.31.98.152	8,193
...	...	...	...
10.255.255.123	8,447	31.31.98.152	8,447

Id. ¶22. But a POSITA would have known that this implementation is inefficient because it stores a large amount of redundant data, and would have further known that the entire table above could be simplified to the following single row:

Private Address	Public Address	Assigned Port Range
10.255.255.123	31.31.98.152	8,192-8,447 ⁶

Id. ¶22. In fact, the latter table is exactly what Fangman claims: “the Service Gateway perform[s] network address persistent port translation (NAPPT)” by “storing translation information in a data structure, wherein the translation information comprises” (1) “the private source IP address of the IP telephone,” (2) “a public address of the Service Gateway,” and (3) “the assigned ports for the IP telephone.” EX1024, 32:48-57. Thus, although perhaps feasible, the Board’s interpretation is inconsistent with Fangman and otherwise would not have been adopted by a POSITA because it is inefficient. EX1039 ¶¶22-23.

Even if the Board were to conclude that Fangman teaches the individual-port implementation and not the port-range implementation, then a POSITA would have at the very least found it obvious to implement the port-range table instead. *Id.* ¶23. As discussed above, a POSITA would have understood that the port-range implementation saves memory over the needlessly inefficient individual-port implementation and could also be used to route inbound data packets based on Fangman’s teachings. *Id.*; *see, e.g.*, EX1024, 3:53-64 (“The Media Gateway Controller may be operable to use the public IP address **and the port range** to

⁶ If implementing a port mask instead of a port range, then this cell would contain the appropriate port mask.

determine the private IP address, for example, by using look-up tables.” (emphasis added)).

2. As the Board Has Already Recognized, a POSITA Would Have Found It Obvious to Combine Fangman with Kumar

Patent Owner's cursory attack on the motivation to combine Fangman with Kumar ignores the multiple motivations to combine articulated in the petition and overstates Kumar. As Petitioner explained, a POSITA would have had several motivations to combine Fangman and Kumar. Petition 46-47. Patent Owner does not address any of these motivations in its response. *See* POR 25–27. Patent Owner argues only that (1) Kumar's larger system is directed to packet classification, not IP telephony, and (2) “Petitioner also has not explained how the system of Kumar would provide any benefit to the IP telephony system of Fangman” because “Kumar describes a complex hierarchical data structure” that “adds significant processing demands that would burden Fangman's NAPPT system.” *Id.* 26–27.

The first argument rests on a fictitious distinction; Kumar expressly discloses that its teachings can be implemented on systems like Fangman's, and Fangman itself teaches using masks in similar contexts. As the name suggests, the IP telephony in Fangman operates via the Internet Protocol, which uses data packets to communicate information. *See* EX1024, 1:14-23, 6:35-39. Kumar's system can also be implemented via the Internet Protocol, (*see* EX1023, 3:22-29), and Kumar further explains that its disclosures “are generally applicable to any device, system, and/or

circumstance where classification of packets or other communications is needed,” (EX1023, 3:22-29). Here, Fangman’s port ranges are used to analyze data packets and determine where to route them, just like the port masks in Kumar. EX1023, 7:31-38, Fig. 7B. Fangman also teaches using masks in a similar context—identifying subnets. Fangman explains that the service gateway can implement subnet masks, (EX1024, 8:60-9:3, 11:25), which are binary masks used to extract relevant portions of a destination IP address from a data packet and then route the data packet, (EX1046, 28-33), just like the ’369 patent’s port masks. Instead of addressing these disclosures head on, Patent Owner hand waives that “Kumar does not address the complexities or processes involved with IP telephony,” but Patent Owner fails to identify these so-called “complexities” or how they would affect the combination. POR 26.

Patent Owner’s second argument is also wrong—contrary to Patent Owner’s assertion that “Petitioner also has not explained how the system of Kumar would provide any benefit to the IP telephony system of Fangman,” (POR 26), Petitioner and its expert did identify benefits of implementing Kumar’s port masks. For example, Petitioner explained that “[a] POSITA would have been aware that masks could be used to determine whether a number lies within a range” and that masks can “optimize performance” of data packet classification and routing. Petition 46. Petitioner’s expert, Dr. Bhattacharjee, expanded on these points, saying that “the use

of masks to determine whether a number falls within a range was ubiquitous in computer networking” and that “a POSITA would have recognized that Kumar’s port masks are computationally efficient because they use only bitwise operations, like logical ANDs” such that “an inclusion in the range can be efficiently computed with one logical operation and a comparison to zero.” EX1003, ¶¶158-59; *see also* EX1003, ¶¶41-51 (describing the benefits of masks in more detail). Patent Owner does not deny, or even address, any of these points. Regardless, “[i]t’s not necessary to show that a combination is ‘the *best* option, only that it be a *suitable* option,” which Petitioner has done. *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 800 (Fed. Cir. 2021) (quoting *PAR Pharm., Inc. v. TWI Pharms., Inc.*, 773 F.3d 1186, 1197-98 (Fed. Cir. 2014)).

Further, Patent Owner’s second argument overstates Kumar. Kumar’s entire system or even its “forest of hash tables” does not need to be implemented into Fangman, just its disclosure of using port masks to classify and route inbound data packets. Petition 45. The Board made this very point in its institution decision: “Patent Owner focuses on specific details of the packet classification system of Kumar, whereas Petitioner relies on the combination of Biswas⁷ and Kumar.” ID

⁷ The Board applied this same reasoning to the combination of Fangman and Kumar. ID 20.

13. “The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference.... Rather, the test is what the combined teachings of those references would have suggested to those of ordinary skill in the art.” *Id.* 13-14 (quoting *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)). A POSITA would have therefore “known to use the masking techniques exemplified by Kumar to implement the disclosed operation.” *Id.* 14.

* * *

Claims 1-6 and 15 are therefore invalid as obvious under grounds 2 and 4.

C. Grounds 3 and 5: A POSITA Would Have Found It Obvious to Apply King's Outbound Teachings to Inbound Communications

1. Patent Owner Recognizes That King Uses Port Ranges to Identify User Devices and Provides No Reason Why This Teaching Is Limited to Outbound Communications

Patent Owner admits King teaches that a device external to the private network can use port ranges to “identify[] a source device” when routing outbound transmissions. POR 27. Patent Owner's primary response, though, is that King does not apply this teaching to inbound transmissions. *Id.* 27-31.

A POSITA would have understood that King's outbound disclosures can easily be applied to routing inbound transmissions and that King's disclosures actually teach toward that idea. EX1039 ¶¶25-29. In fact, contrary to Patent Owner's argument that nothing “suggests that the above method could function in reverse,” (POR, 30), a POSITA would have understood that applying this exact

identification process to inbound data packets would be trivial, (EX1039 ¶26). Instead of comparing the source port of a received data packet to the stored port range, it would have been obvious to just compare the destination port. EX1039 ¶26. In terms of code, this amounts to simply changing one variable in a function or SQL query: “received_source_port” to “received_destination_port.” *Id.*

In fact, King teaches toward this very idea. *Id.* ¶27. The background section of King discusses Port Address Translation (“PAT”), which is a process for routing both outbound *and inbound* data packets. EX1025, 2:62-3:6. King explains that the problem with PAT, however, is that “it is not possible for a provider edge device such as an aggregation device to classify incoming packets as belonging to a particular host or user device without additional information being provided.” *Id.* 3:47-50. King therefore proposes supplementing or replacing PAT with its invention. *Id.* 3:67-4:2, 5:33-35. A POSITA would have known that, to replace or supplement PAT, King’s invention would be performed on both outbound and inbound data packets. EX1039 ¶27. King recognizes as much, when it explains that “[t]he aggregation device obtains an applies a policy to communication *between* the user device and the Internet”—not just *from* the user device *to* the Internet—to ensure “that an appropriate quality of service (QoS) such as bandwidth is applied and that an appropriate billing method is applied” and/or “to exert parental control

on content”—which are policies that would need to be applied to both outbound and inbound transmissions. EX1025, 1:21-33 (emphasis added), 3:53-59.

Further, a POSITA would have recognized that aggregation device **110** must know where to send inbound data packets, especially when servicing “multiple CPEs” that “reuse [] a common IP address.” EX1039 ¶28; EX1025, 2:29-34; *see also* EX1025, 1:25-28 (“One or more CPE’s communicate with a gateway to the network such as an aggregation device.”). A POSITA would have understood that aggregation device **110** could use NAT or PAT to route these inbound data packets—as in the prior-art method described in King, (EX1025, 2:13-39)—but a POSITA would have known that implementing NAT or PAT would needlessly waste resources—for example, memory—because the aggregation device **110** can already identify internal devices by comparing the received port number to the stored port-range assignments, (EX1039 ¶28). A POSITA would have therefore known to use King’s port-range disclosure to route inbound data packets. EX1039 ¶28.

Patent Owner’s argument that King does not disclose routing an inbound data packet based on an identifier is technically unsound. POR 31-33. Patent Owner does not explain how aggregation device **110** could route an inbound data packet to a user device without using the user device’s private address, *i.e.*, the identifier. EX1039 ¶29. The global address is not sufficient, especially if the aggregation device is servicing multiple CPEs and user devices, because the global address is not unique

to any one of these devices. *Id.* That would be like trying to send a letter to a specific person—*e.g.*, “John Smith”—by addressing the letter to a general entity that is not unique to that person—*e.g.*, “Connecticut” or “Corporate Headquarters.” *Id.* The aggregation device **110** would need to use something more specific, like the user device’s identifier. *Id.* Thus, a POSITA would have found it obvious to use the identifier to route inbound data packets for the reasons articulated in the petition. Petition 53-64.

Accordingly, a POSITA would have recognized that King’s invention is applicable to both outbound and inbound transmissions, and would have further understood that King does not need to detail the inbound process because it is functionally identical to the outbound process. EX1039 ¶¶25-29.

2. As the Board Has Already Recognized, a POSITA Would Have Found It Obvious to Combine King with Kumar

Patent Owner makes the same attacks here that it did for the combination of Fangman and Kumar. For the reasons discussed above, Patent Owner’s argument is unconvincing, and a POSITA would have been motivated to combine King and Kumar. *See supra* § II.B.2; Petition 59-60.

* * *

Claims 1-6 and 15 are therefore invalid as obvious under grounds 3 and 5.

III. CONCLUSION

For the reasons above and in Petitioner's petition, the Board should find all claims of the '369 patent unpatentable.

Date: October 22, 2024

By: /s/ Todd M. Briggs

James M. Glass (Reg. No. 46,729)
jimglass@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
51 Madison Ave., 22nd Floor
New York, New York 10010
Tel: (212) 849-7000
Fax: (212) 849-7100

Todd M. Briggs (Reg. No. 44,040)
toddbriggs@quinnemanuel.com
Kevin Johnson (Reg. No. 38,927)
kevinjohnson@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Tel: (650) 801-5000
Fax: (650) 801-5100

Nima Hefazi (Reg. No. 63,658)
nimahefazi@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Tel: (213) 443-3000
Fax: (213) 443-3100

Attorneys for Petitioner Juniper Networks, Inc.

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Petitioner hereby certifies, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Reply, that the number of words in this paper is 5,544. Pursuant to 37 C.F.R. §42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under §42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Date: October 22, 2024

Respectfully submitted,

By: /s/ Todd M. Briggs
Todd M. Briggs

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing Petitioner's Reply to Patent Owner Response was served via e-mail pursuant to 37 C.F.R. §42.6(e) in its entirety to all counsel of record, as follows:

R. Allan Bullwinkel (Reg. No. 77,630)
abullwinkel@hpcllp.com
Michael F. Heim (Reg. No. 32,702)
mheim@hpcllp.com
Christopher L. Limbacher (Reg. No. 76,551)
climbacher@hpcllp.com
William B. Collier, Jr. (*pro hac vice*)
wcollier@hpcllp.com
Heim Payne & Chorush, LLP
609 Main Street, Suite 3200
Houston, TX 77002
Telephone: 713-221-2000
Facsimile: 713-221-2021

DATED: October 22, 2024

Respectfully submitted,

By: /s/ Todd M. Briggs
Todd M. Briggs